

1 **Listing of Claims:**

2  
3 This listing of claims will replace all prior versions, and listings, of claims in the application.

4 1. - 8. (Canceled).

5  
6 9. - 16. (Canceled).

7  
8 17. - 154. (Canceled).

9  
10 155. (Canceled)

11  
12 156. (Canceled).

13  
14 157. - 161. (Canceled).

15  
16 162. (Canceled).

17  
18 163. - 182. (Canceled).

19  
20 183. Canceled.

21  
22 184. (Previously presented) The method as recited in claim 258 wherein said step of sending  
23 recipient data for confirming proper delivery of said e-mail includes the steps of:

24 a) generating a confirmation of receipt notice wherein the inputted recipient data is included with  
25 said confirmation of receipt notice; and

1 b) sending said confirmation of receipt notice, wherein the inputted recipient data included with  
2 said confirmation of receipt notice can be compared to information associated with said intended  
3 recipient in order to verify whether the e-mail was accessed by the intended recipient.

4  
5 185. (Previously presented) The method as in claim 236, wherein said access event comprises  
6 access of said e-mail that was delivered to said recipient e-mail address.

7  
8 186. (Previously presented) The method as in claim 236, wherein said access event comprises  
9 access of an e-mail account associated with said recipient e-mail address.

10  
11 187. (Previously presented) The method as in claim 236, wherein said access event comprises  
12 activation of an e-mail processing software associated with said recipient e-mail address.

13  
14 188. (Previously presented) The method as in claim 236, wherein the step of transmitting an e-  
15 mail from a sender computer includes attaching an executable attachment file in conjunction with  
16 the e-mail, the executable attachment file having a first module for prompting the party who  
17 requested said access event to enter recipient data; and

18 and wherein the step of detecting an access event includes the step of executing the first  
19 module of the executable attachment file.

20  
21 189. (Previously presented) The method as in claim 188, wherein the executable attachment  
22 file has a second module transmitted and delivered therewith, the second module for detecting the  
23 access event, and further comprising the step of automatically executing the second module upon  
24 delivery of the attachment file to the recipient e-mail address.

25  
26 190. (Canceled).

1 191. (Previously presented) The method as in claim 236, wherein said recipient e-mail address  
2 is associated with a recipient computer.

3  
4 192. (Previously presented) The method as in claim 191, wherein said recipient computer is a  
5 server of a service provider.

6  
7 193. (Previously presented) The method as in claim 191, wherein said recipient computer is a  
8 user system that is directly accessible by a recipient, said user system including electronic mail  
9 processing software.

10  
11 194. (Previously presented) The method as in claim 236, wherein said inputted recipient data  
12 pertains to alphanumeric text identification, biometric identification, password identification, a  
13 computer generated user code, or a combination thereof.

14  
15 195. (Previously presented) The method as in claim 236, wherein said inputted recipient data  
16 comprises identity information that identifies an individual.

17  
18 196. (Previously presented) The method as in claim 195, wherein said identity information  
19 pertains to biometric identification.

20  
21 197. (Previously presented) The method as in claim 196 further comprising the step of  
22 recognizing biometric attributes of an individual.

23  
24 198. (Previously presented) The method as in claim 195, wherein said identity information  
25 includes alphanumeric text identification information.

1 199. (Previously presented) The method as in claim 236 , wherein said inputted recipient data  
2 comprises information that identifies a business.

3  
4 200. (Previously presented) The method as in claim 236, wherein said inputted recipient data  
5 comprises information that identifies an organization.

6  
7 201. (Previously presented) The method as in claim 236 , wherein said inputted recipient data  
8 comprises a computer generated user code.

9  
10 202. (Previously presented) The method as in claim 236 further including the step of sending  
11 access event data of attendant conditions of said access event.

12  
13 203. (Previously presented) The method as in claim 236 , wherein said recipient is an  
14 individual.

15  
16 204. (Previously presented) The method as in claim 236, wherein said recipient is a business.

17  
18 205. (Previously presented) The method as in claim 236, wherein said recipient is an  
19 organization.

20  
21 206. (Previously presented) The method as in claim 236, wherein said inputted recipient data  
22 is used to verify proper delivery of legal documents.

23  
24 207. (Previously presented) The method as in claim 236, wherein said inputted recipient data  
25 is used to verify proper delivery of confidential documents.

1 208. (Previously presented) The method recited by claim 260 wherein said step of sending  
2 recipient data for confirming proper delivery of said e-mail includes the steps of:

3 a) generating a confirmation of receipt notice wherein the acquired recipient data is  
4 included with said confirmation of receipt notice; and

5 b) sending said confirmation of receipt notice, wherein the acquired recipient data  
6 contained with said confirmation of receipt notice can be compared to information associated with  
7 said intended recipient in order to verify whether the email was accessed by the intended recipient.  
8

9 209. (Previously presented) The method as in claim 260, wherein said access event comprises  
10 access of said e-mail that was delivered to said recipient e-mail address.  
11

12 210. (Previously presented) The method as in claim 260, wherein said access event comprises  
13 access of an e-mail account associated with said recipient e-mail address.  
14

15 211. (Previously presented) The method as in claim 260, wherein said access event comprises  
16 activation of e-mail processing software associated with said recipient e-mail address.  
17

18 212. (Previously presented) The method as in claim 260, wherein the step of transmitting an e-  
19 mail from a sender computer includes attaching an executable attachment file in conjunction with  
20 the e-mail, the executable attachment file having a first module for acquiring recipient data that is  
21 related to biometric identification of the recipient, and

22 wherein the step of detecting an access event includes the step of executing the first module  
23 of the executable attachment file.  
24  
25  
26  
27

1 213. (Previously presented) The method as in claim 212, wherein the executable attachment  
2 file has a second module transmitted and delivered therewith, the second module for detecting the  
3 access event, and further comprising the step of:

4 automatically executing the second module upon delivery of the attachment file to the  
5 recipient e-mail address.

6  
7 214. Canceled.

8  
9 215. (Previously presented) The method as in claim ~~208~~ 260, wherein said recipient e-  
10 mail address is associated with a recipient computer.

11  
12 216. (Previously presented) The method as in claim 215, wherein said recipient computer  
13 is a server of a service provider that is capable of receiving e-mail.

14  
15 217. (Previously presented) The method as in claim 215, wherein said recipient computer  
16 is a user system that is directly accessible by the recipient, said user system including electronic  
17 mail processing software and being capable of receiving e-mail.

18  
19 218. (Previously presented) The method as in claim 260, wherein said acquired recipient  
20 data is related to a biometric imprint, alphanumeric text identification, password identification, a  
21 computer generated user code, or a combination thereof.

22  
23 219. (Previously presented) The method as in claim 260, wherein said acquired recipient  
24 data comprises identity information that identifies an individual.

1 220. (Previously presented) The method as in claim 260 further comprising means for  
2 recognizing biometric attributes of an individual.

3  
4 221. (Previously presented) The method as in claim 260, wherein said acquired recipient  
5 data comprises information that identifies a business.

6  
7 222. (Previously presented) The method as in claim 260, wherein said acquired recipient  
8 data comprises information that identifies an organization.

9  
10 223. (Previously presented) The method as in claim 260, wherein said acquired recipient  
11 data comprises a computer generated user code.

12  
13 224. (Previously presented) The method as in claim 260 further including the step of  
14 sending access event data of conditions attendant said access event.

15  
16 225. (Previously presented) The method as in claim 260, wherein said recipient is an  
17 individual.

18  
19 226. (Previously presented) The method as in claim 260, wherein said recipient is a  
20 business.

21  
22 227. (Previously presented) The method as in claim 260, wherein said recipient is an  
23 organization.

24  
25 228. (Previously presented) The method as in claim 260, wherein said sent recipient data  
26 is used to verify proper delivery of legal documents.

1 229. (Previously presented) The method as in claim 260, wherein said sent recipient data is used  
2 to verify proper delivery of confidential documents.

3  
4 230. (Canceled).

5  
6 231. (Previously presented) The method as in claim 260, wherein said recipient data is  
7 acquired as a requisite condition for permitting access to said delivered e-mail.

8  
9 232. (Previously presented) The method as in claim 260, wherein said recipient data is  
10 acquired as a requisite condition for permitting access to said recipient e-mail address.

11  
12 233. (Previously presented) The method as in claim 260, wherein said recipient data is  
13 acquired as a requisite condition for operating a remote user computer, said remote user computer  
14 being operable to gain access to said recipient e-mail address.

15  
16 234. (Previously presented) The method as in claim 260, wherein said recipient data is  
17 comprised of alphanumeric text, said alphanumeric text being associated with the at least one  
18 biometric attribute of said recipient.

19  
20 235. (Canceled).

21  
22 236. (Previously presented) A method for verifying whether an e-mail sent by a sending  
23 party was accessed by an intended recipient, said method comprising:

24 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
25 computer being connected to a communications network;

26 b) delivering said e-mail to a recipient e-mail address;

27



1 c) detecting an access event, and prompting the party associated with said access event to  
2 input recipient data prior to allowing the requested access, said recipient data including identifying  
3 data related to the party associated with said requested access; and

4 d) sending recipient data for confirming proper delivery of said e-mail.

5  
6 237. (Previously presented) The method recited by claim 264 wherein the step of sending data  
7 that identifies said recipient for confirming proper delivery of said e-mail includes the steps of :

8 a) generating a confirmation of receipt notice wherein the data that identifies the recipient  
9 is included with said confirmation of receipt notice; and

10 b) sending said confirmation of receipt notice, wherein the data that identifies the recipient  
11 that is included with said confirmation of receipt notice can be compared to information associated  
12 with said intended recipient in order to verify whether the email was accessed by the intended  
13 recipient.

14  
15 238. (Previously presented) The method as in claim 264, wherein said data that identifies  
16 said recipient is related to a biometric imprint, alphanumeric text identification, password  
17 identification, a computer generated user code, or a combination thereof.

18  
19 239. (Previously presented) The method as in claim 264, wherein the data that identifies  
20 said recipient is comprised of alphanumeric text, said alphanumeric text being associated with the at  
21 least one biometric attribute of said recipient.

22  
23 240. (Previously presented) The method as in claim 264 further including the step of  
24 recognizing biometric attributes of an individual.

1 241. (Previously presented) The method as in claim 264, wherein said data that identifies  
2 said recipient comprises identity information that identifies an individual.

3  
4 242. (Previously presented) The method as in claim 264, wherein said data that identifies  
5 said recipient comprises information that identifies a business.

6  
7 243. (Previously presented) The method as in claim 264, wherein said data that identifies  
8 said recipient comprises information that identifies an organization.

9  
10 244. - 247. (Canceled).

11  
12 248. (Previously presented) A system for verifying whether e-mail sent by a sending party  
13 was accessed by an intended recipient, said system comprising:

14 a) a sender computer connected to a communications network and from which an e-  
15 mail is transmitted;

16 b) a recipient computer connected to said communications network, said recipient  
17 computer capable of receiving said transmitted e-mail and further having data storage means for  
18 storing said received e-mail;

19 c) software capable of detecting an access event, wherein, upon detecting said access  
20 event, said software prompts the party associated with said access event to input recipient data prior  
21 to allowing the requested access, said recipient data comprising identifying data related to the party  
22 associated with said requested access; and

23 d) means for sending recipient data for confirming proper delivery of said e-mail.

24  
25 249. (Previously presented) The system as in claim 248, wherein said access event comprises  
26 access of a delivered e-mail.

1 250. (Previously presented) The system as in claim 248, wherein said access event  
2 comprises access of an e-mail account associated with the e-mail address to which said e-mail was  
3 delivered.

4  
5 251. (Previously presented) The system as in claim 248, wherein said access event  
6 comprises activation of the e-mail processing software associated with the e-mail address to which  
7 said e-mail was delivered.

8  
9 252. (Previously presented) A system for verifying whether e-mail sent by a sending party  
10 was accessed by an intended recipient, said system comprising:

11 a) a sender computer connected to a communications network and from which an e-mail is  
12 transmitted;

13 b) a recipient computer connected to said communications network, said recipient  
14 computer being capable of receiving said transmitted e-mail and further having data storage means  
15 for storing said received e-mail;

16 c) biometric identification means for recognizing biometric attributes of an individual;

17 d) software capable of detecting an access event and identifying an individual through  
18 utilization of inputted biometric attributes of said individual; and

19 e) means for sending data that identifies said individual for confirming proper delivery of  
20 said e-mail.

21  
22 253. (Previously presented) The system as in claim 252, wherein said access event  
23 comprises access of a delivered e-mail.

1 254. (Previously presented) The system as in claim 252, wherein said access event  
2 comprises access of an e-mail account associated with the e-mail address to which said e-mail was  
3 delivered.

4  
5 255. (Previously presented) The system as in claim 252, wherein said access event comprises  
6 activation of the e-mail processing software associated with the e-mail address to which said e-mail  
7 was delivered.

8  
9 256. - 257. (Canceled).

10  
11 258. (Previously presented) A method for verifying whether an e-mail sent by a sending  
12 party was accessed by an intended recipient, said method comprising:

- 13 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
14 computer being connected to a communications network;  
15 b) delivering said e-mail to an e-mail address;  
16 c) detecting an access event, and prompting the party that requested said access to input  
17 recipient data prior to allowing the requested access, said recipient data including identifying data  
18 that is associated with the party that requested said access; and  
19 d) sending recipient data for confirming proper delivery of said e-mail.

20  
21 259. (Previously presented) The method recited by claim 236 wherein said step of sending  
22 recipient data for confirming proper delivery of said e-mail includes the steps of:

- 23 a) generating a confirmation of receipt notice wherein the inputted recipient data is included  
24 with said confirmation of receipt notice; and  
25  
26  
27

1           b) sending said confirmation of receipt notice, wherein the inputted recipient data included  
2 with said confirmation of receipt notice can be compared to information associated with said  
3 intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

4  
5 260. (Previously presented) A method for verifying whether e-mail sent by a sending party was  
6 accessed by an intended recipient, said method comprising:

7           a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
8 computer being connected to a communications network;

9           b) delivering said e-mail to a recipient e-mail address;

10           c) detecting an access event;

11           d) acquiring recipient data that is related to biometric identification of the recipient; and

12           e) sending recipient data for confirming proper delivery of said e-mail.

13  
14 261. (Previously presented) The method as recited in claim 260 wherein said recipient data is  
15 acquired prior to said access event.

16  
17 262. (Previously presented) The method as recited in claim 260 wherein said recipient data is  
18 acquired after said access event.

19  
20 263. (Previously presented) The method as recited in claim 260 wherein said recipient data is sent  
21 to an e-mail address.

22  
23 264. (Previously presented) A method for verifying whether e-mail sent by a sending party was  
24 accessed by an intended recipient, said method comprising:

25           a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
26 computer being connected to a communications network;

- 1 b). delivering said e-mail to an e-mail address;
- 2 c) identifying a recipient utilizing biometric identification;
- 3 d) detecting an access event; and
- 4 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

5  
6 265. (Previously presented) The method as recited in claim 264 wherein said recipient is  
7 identified prior to said access event.

8  
9 266. (Previously presented) The method as recited in claim 264 wherein said recipient is identified  
10 after said access event.

11  
12 267. (Previously presented) The method as recited in claim 264 wherein said data that identifies  
13 said recipient is sent to an e-mail address.

14  
15 268. (Previously presented) A method for verifying whether e-mail sent by a sending party was  
16 accessed by an intended recipient, said method comprising:

- 17 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
18 computer being connected to a communications network;
- 19 b) delivering said e-mail to an e-mail address;
- 20 c) identifying a recipient in association with biometric identification;
- 21 d) detecting an access event; and
- 22 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

23  
24 269. (Previously presented) The method as in claim 268 wherein said recipient is identified prior  
25 to said access event.

1 270. (Previously presented) The method as in claim 268 wherein said recipient is identified after  
2 said access event.

3  
4 271. (Previously presented) The method as in claim 268 wherein said data that identifies said  
5 recipient is sent to an e-mail address.

6  
7 272. - 278. (Canceled).

8  
9 279. (Previously presented) The system as in claim 252, wherein said data that identifies said  
10 individual for confirming proper delivery of said e-mail is sent to an e-mail address.

11  
12 280. - 287. (Canceled).

13  
14 288. (Previously presented) The method as in claim 287, wherein said confirmation of receipt  
15 notice is sent to an e-mail address.

16  
17 289. (Previously presented) The method as in claim 272, wherein said access event  
18 comprises access of said e-mail that was delivered to said recipient e-mail address.

19  
20 290. (Previously presented) The method as in claim 272, wherein said access event comprises  
21 access of an e-mail account associated with said recipient e-mail address.

22  
23 291. (Previously presented) The method as in claim 272, wherein said access event comprises  
24 activation of an e-mail processing software associated with said recipient e-mail address.

1 292. (Previously presented) The method as in claim 272, wherein the step of transmitting  
2 an e-mail from a sender computer includes attaching an executable attachment file in conjunction  
3 with the e-mail file, the executable attachment file having a first module for discovering the stored  
4 recipient data that is associated with said recipient, and wherein the step of detecting an access  
5 event includes the step of executing the first module of the executable attachment.

6  
7 293. (Previously presented) The method as in claim 292, wherein the executable  
8 attachment file has a second module transmitted and delivered therewith, the second module for  
9 detecting the access event, and further comprising the step of:

10 automatically executing the second module upon delivery of the attachment file to said  
11 recipient e-mail address.

12  
13 294. (Previously presented) The method as in claim 272, wherein said recipient e-mail  
14 address is associated with a recipient computer.

15  
16 295. (Previously presented) The method as in claim 294, wherein said recipient computer  
17 is a server of a service provider.

18 296. (Previously presented) The method as in claim 294, wherein said recipient computer is a  
19 user system that is directly accessible by a recipient, said user system including electronic mail  
20 processing software.

21  
22 297. (Previously presented) The method as in claim 272, wherein a remote user computer  
23 may be used to gain remote access to said recipient e-mail address.



1 298. (Previously presented) The method as in claim 272, wherein said computer on which said  
2 recipient data is stored is a recipient computer.

3  
4 299. (Previously presented) The method as in claim 272, wherein said computer on which said  
5 recipient data is stored is a remote user computer.

6  
7 300. (Previously presented) The method as in claim 272, wherein said recipient data is contained  
8 in a data file, said data file being stored on said storage element of said computer.

9  
10 301. (Previously presented) The method as in claim 272, wherein said storage element comprises  
11 of a hard disk drive.

12  
13 302. (Previously presented) The method as in claim 272, wherein said storage element comprises  
14 of a memory module.

15  
16 303. (Previously presented) The method as in claim 272, wherein recipient data pertaining to said  
17 recipient of e-mail is stored on said storage element prior to said access event.

18  
19 304. (Previously presented) The method as in claim 272, wherein said stored recipient data  
20 pertains to alphanumeric text identification, biometric identification, password identification, a  
21 computer generated user code, or a combination thereof.

22  
23 305. (Previously presented) The method as in claim 272, wherein said stored recipient data  
24 comprises identity information that identifies an individual.

1 306. (Previously presented) The method as in claim 305, wherein said identity information  
2 pertains to biometric identification.

3  
4 307. (Previously presented) The method as in claim 306 further comprising the step of  
5 recognizing biometric attributes of an individual.

6  
7 308. (Previously presented) The method as in claim 305, wherein said identity information  
8 includes alphanumeric text identification data.

9  
10 309. (Previously presented) The method as in claim 272, wherein said stored recipient  
11 data includes information that identifies a business.

12  
13 310. (Previously presented) The method as in claim 272, wherein said stored data includes  
14 information that identifies an organization.

15  
16 311. (Previously presented) The method as in claim 272, wherein said stored recipient data  
17 includes a computer generated user code.

18  
19 312. (Previously presented) The method as in claim 272 further including the step of  
20 sending access event data of attendant conditions of said access event.

21  
22 313. (Previously presented) The method as in claim 272, wherein said recipient is an  
23 individual.

24  
25 314. (Previously presented) The method as in claim 272, wherein said recipient is a business.  
26  
27

1 315. (Previously presented) The method as in claim 272, wherein said recipient is an  
2 organization.

3  
4 316. (Previously presented) The method as in claim 272, wherein said sent recipient data  
5 is used to verify proper delivery of legal documents.

6  
7 317. (Previously presented) The method as in claim 272, wherein said sent recipient data  
8 is used to verify proper delivery of confidential documents.

9  
10 318. - 326. (Canceled).

11  
12 327. (Previously presented) The method as in claim 236, wherein said recipient data for  
13 confirming proper delivery of said e-mail is sent to an e-mail address.

14  
15 328. (Previously presented) The method as in claim 236, wherein a remote user computer may  
16 be used to gain remote access to said recipient e-mail address.

17  
18 329. (Previously presented) The method as in claim 236 wherein the party that is associated with  
19 said access event is an individual.

20  
21 330. (Previously presented) The method as in claim 236 wherein the party that is associated with  
22 said access event is a business.

23  
24 331. (Previously presented) The method as in claim 236 wherein the party that is associated with  
25 said access event is an organization.

1 332. (Previously presented) The method as in claim 258 wherein said recipient data for  
2 confirming proper delivery of said e-mail is sent to an e-mail address.

3  
4 333. (Previously presented) The method as in claim 184, wherein said confirmation of receipt  
5 notice is sent to an e-mail address.

6  
7 334. (Previously presented) The method as in claim 258, wherein said inputted recipient data  
8 pertains to alphanumeric text identification, biometric identification, password identification, a  
9 computer generated user code, or a combination thereof.

10  
11 335. (Previously presented) The method as in claim 208, wherein said confirmation of receipt  
12 notice is sent to an e-mail address.

13  
14 336. (Previously presented) The method as in claim 260, wherein a remote user computer may be  
15 used to gain remote access to said recipient e-mail address.

16  
17 337. (Previously presented) The method as in claim 219, wherein said identity information  
18 includes alphanumeric text identification.

19  
20 338. (Previously presented) The method as in claim 237, wherein said confirmation of receipt  
21 notice is sent to an e-mail address.

22  
23 339. (Previously presented) The method as in claim 268, wherein said data that identifies  
24 said recipient is related to a biometric imprint, alphanumeric text identification, password  
25 identification, a computer generated user code, or a combination thereof.

1 340. (Previously presented) The method as in claim 268 further comprising the step of  
2 recognizing biometric attributes of an individual.

3  
4 341. - 345. (Canceled).

5  
6 346. (Previously presented) The system as in claim 248, wherein said recipient data for  
7 confirming proper delivery of said e-mail is sent to an e-mail address.

8  
9 347. (Previously presented) The system as in claim 252, wherein said individual is identified  
10 prior to said access event.

11  
12 348. (Previously presented) The system as in claim 252, wherein said individual is identified  
13 after said access event.